PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-339236
(43)Date of publication of application : 08.12.2000

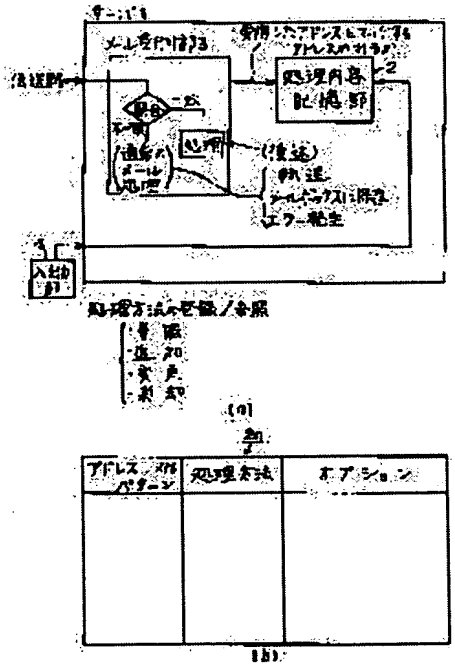
(51)Int.Cl. G06F 13/00

(21)Application number : 11-147680
(22)Date of filing : 27.05.1999

(71)Applicant : FUJITSU LTD
(72)Inventor : UEDA HARUYASU

(54) MISCHIEVOUS MAIL PREVENTING DEVICE, METHOD THEREFOR AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the device and method capable of preventing reception of a mischievous mail.
SOLUTION: Plural transmitting destinations with parts which can be optionally decided by a user are received as the transmitting destinations for each user, when a mail is received from a transmission line, a transmitting address is extracted from the mail at a mail accepting part 3 and collected with an address or an address pattern stored in a table 2a of a processed contents storage part 2 by a server 1 to distribute an electronic mail. When they are not matched with each other, a normal mail processing to the user is performed, and when they are matched with each other, a processing such as cancellation of the mail, return of an error mail, attachment of a mark on a specified area of the mail, addition of the address of the transmitting destination, according to the nature of the mail is performed. Otherwise, when a ciphered pattern is included in the address, a processing according to a command obtained by decoding the pattern is performed.



LEGAL STATUS

[Date of request for examination] 29.10.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－339236
（P2000－339236A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｇ　５Ｂ０８９

審査請求　未請求　請求項の数18　ＯＬ　（全 17 頁）

(21)出願番号　特願平11－147680

(22)出願日　平成11年５月27日(1999.5.27)

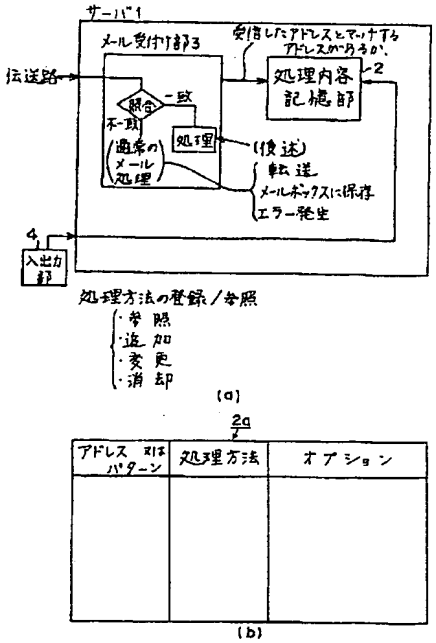
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　上田　晴康
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100074099
弁理士　大菅　義之　（外１名）

Ｆターム(参考)　5B089 GA11 GA21 GB02 JA31 KA12 KB06 KC23 KC27 KC34 KC53 KC59 LA14 LA15 MD07

(54)【発明の名称】　悪戯メール防止装置、その方法及び記録媒体

(57)【要約】
【課題】悪戯メールの受信を防止することのできる装置及び方法を提供する。
【解決手段】電子メールを配信するサーバ１は、各ユーザのための送信先として、ユーザが任意に決められる部分を持つ複数の送信先を受信する事ができ、伝送路からメールを受信すると、メール受け付け部３において、メールから送信アドレスを抽出し、それを処理内容記憶部２のテーブル２ａに記憶されているアドレスあるいはアドレスパターンと照合する。一致しない場合には、そのユーザへの通常のメール処理を行い、一致する場合には、メールを破棄する、エラーメールを返送する、メールの所定領域に目印を添付する、送信先のアドレスを付加する、メールの有する性質に従った処理を行う。あるいは、アドレスに暗号化されたパターンが含まれている場合には、該パターンを復号して得られたコマンドに従った処理を行う。

本発明の第１の実施形態を示す図



1

【特許請求の範囲】

【請求項１】悪戯メールを防止する装置であって、
受信した電子メールからメールアドレスを抽出するメールアドレス抽出手段と、
特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録する記憶手段と、
該受信した電子メールのメールアドレスと該記憶手段に記憶されているメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するメール処理手段と、を備えることを特徴とする装置。

【請求項２】特定の性質を持ったメールとそれ以外のメールを区別して処理するよう指定する指定手段を更に備えることを特徴とする請求項１に記載の装置。

【請求項３】暗号化された処理方法を解釈して処理する手段を更に備えることを特徴とする請求項１に記載の装置。

【請求項４】電子メールを受信する受信手段と、受信した全ての電子メールを、送信元のアドレスを付加して配信する手段とを備える電子メールサーバから電子メールを受信する装置であって、
受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対する処理方法を設定する手段を備えることを特徴とする装置。

【請求項５】特定の性質を持ったメールとそれ以外のメールを区別して処理するよう指定する指定手段を更に備えることを特徴とする請求項８に記載の装置。

【請求項６】暗号化された処理方法を解釈して処理する手段を更に備えることを特徴とする請求項４に記載の装置。

【請求項７】電子メールを送信するときに自分のアドレスとして発行したアドレスを、付加的な情報と関連づけて記録しておき、該付加的な情報を必要に応じて表示することを特徴とする請求項４に記載の装置。

【請求項８】前記電子メールの送信時に発行したアドレスと該電子メールの送信相手を記録しておき、その後、該送信相手にメールを送信する際には、自分のアドレスとして該発行したアドレスを使うことを特徴とする請求項４に記載の装置。

【請求項９】悪戯メールを防止する方法であって、
（ａ）受信した電子メールからメールアドレスを抽出するステップと、
（ｂ）特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録するステップと、
（ｃ）該受信した電子メールのメールアドレスと該ステップ（ｂ）で記憶されたメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するステップと、を備えることを特徴とする方法。

2

【請求項１０】特定の性質を持ったメールとそれ以外のメールを区別して処理するよう指定するステップを更に備えることを特徴とする請求項９に記載の方法。

【請求項１１】暗号化された処理方法を解釈して処理するステップを更に備えることを特徴とする請求項９に記載の方法。

【請求項１２】電子メールを受信する受信手段と、受信した全ての電子メールを、送信元のアドレスを付加して配信する手段とを備える電子メールサーバから電子メールを受信する方法であって、
受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対する処理方法を設定するステップを備えることを特徴とする方法。

【請求項１３】特定の性質を持ったメールとそれ以外のメールを区別して処理するよう指定するステップを更に備えることを特徴とする請求項１２に記載の方法。

【請求項１４】暗号化された処理方法を解釈して処理するステップを更に備えることを特徴とする請求項１２に記載の方法。

【請求項１５】電子メールを送信するときに自分のアドレスとして発行したアドレスを、付加的な情報と関連づけて記録しておき、該付加的な情報を必要に応じて表示することを特徴とする請求項１２に記載の方法。

【請求項１６】前記電子メールの送信時に発行したアドレスと該電子メールの送信相手を記録しておき、その後、該送信相手にメールを送信する際には、自分のアドレスとして該発行したアドレスを使うことを特徴とする請求項１２に記載の方法。

【請求項１７】コンピュータに、
（ａ）受信した電子メールからメールアドレスを抽出するステップと、
（ｂ）特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録するステップと、
（ｃ）該受信した電子メールのメールアドレスと該ステップ（ｂ）で記憶されたメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するステップと、を備える処理を実行させるコンピュータ読み取り可能なプログラムを記録している記録媒体。

【請求項１８】電子メールを受信する受信手段と、受信した全ての電子メールに、送信元のアドレスを付加する手段とを備える電子メールサーバから電子メールを受信するコンピュータに、
受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対しての処理方法を設定する

ステップを備える処理を実行させるコンピュータ読み取り可能なプログラムを記録している記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子メールに係り、特に、悪戯メールの防止方法及び防止装置に関する。

【０００２】

【従来の技術】今日、インターネットが一般に普及し、インターネットを介して多くの情報がやりとりされる様になった。情報のやりとりの中には、ホームページによる情報の公開の他に、従来からあった、電子メールでの情報のやりとりがある。ところが、今日では、個人の電子メールアドレスが、予期せぬ相手に漏洩し、不要な電子メールが大量に送られてくるという問題が発生している。従来、ＳＰＡＭと呼ばれる宣伝や悪戯のためのメールの被害を防止するためには、電子メールソフトで対応する必要があった。このような、ＳＰＡＭ防止方法に於いては、ＳＰＡＭにしばしば現れる文字列を検出したり、特定のメールアドレスから送られてくるものを除くことは可能だったが、そのような方法を提供する米国特許５６１９６４８号では、本質的な解決にはならず、ＳＰＡＭ送信の手口がどんどん複雑になって、いたちごっこになるだけであった。

【０００３】また、まれにだが、本来受け取りたいメールをＳＰＡＭと間違えて除いてしまったために読めなくなるという危険もあった。すなわち、同じ文字列を含む電子メールであっても、その文字列の示す内容を勧誘するものと、その文字列で表される内容に対する反対意見を述べるものとがあり、文字列の検出のみによって受信したメールの要／不要を決めるのは、おのずと限界がある。

【０００４】また、電子メールアドレスを教える機会がどんどん増えるにつれ、どこからＳＰＡＭ相手にメールアドレスが知られてしまったのかを追跡することはほとんど不可能であった。すなわち、今日では、個人がホームページを開設し、情報を公衆に向けて発信するということが多くなったが、ホームページに掲載される情報に対する責任の所在を明らかにするために、ホームページへの情報の掲載者のメールアドレスを公開することが行われている。このような場合、メールアドレスが世界中のどのような人に見られているか分からず、悪戯メールが送られてくる可能性も非常に高くなって来ている。

【０００５】なお、電子メールの処理方法は、既に公知であるので、詳細な説明は以下の説明に於いて省略する。電子メールの処理方法の詳細については、例えば、「sendmailシステム管理」Bryan Costales 、Eric Allman著、株式会社オライリー・ジャパン発行、オーム社発売、あるいは、Network Information Center (NIC) から配布されるRFC (Request For Comments) を参照されたい。

【０００６】

【発明が解決しようとする課題】従来のシステムにおいても、自分の電子メールアドレスが、ＳＰＡＭの対象となってることが分かった時点で電子メールアドレスを変更することは不可能ではなかったが、従来のシステムは、電子メールのアドレスは一人につき一つずつ割り当てられており、料金もアドレス一つに付き一定額であることが多いため、ＳＰＡＭによる被害を受けるたびにプロバイダとの契約の変更をしたり、通常使う電子メールアドレスを変更したり、人に教えた電子メールアドレスを変えてもらったりすることは難しく、現実的な方法ではなかった。

【０００７】また、電子メールに関しては発送する側のコストが低いため、メールアドレスさえ知っていれば大量の電子メールを送ることができてしまう。このため、ＳＰＡＭを、何らかの方法で、いずれから収集してきたメールアドレスに向かって一斉に送ることが容易に可能となっている。ＳＰＡＭは、インターネットの普及率が高いアメリカなどでは大問題となっており、日本でも問題になりつつある。

【０００８】本発明の課題は、悪戯メールの受信を防止することのできる装置及び方法を提供することである。

【０００９】

【課題を解決するための手段】本発明の第１の側面における装置は、悪戯メールを防止する装置であって、受信した電子メールからメールアドレスを抽出するメールアドレス抽出手段と、特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録する記憶手段と、該受信した電子メールのメールアドレスと該記憶手段に記憶されているメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するメール処理手段とを備えることを特徴とする。

【００１０】本発明の第２の側面における装置は、電子メールを受信する受信手段と、受信した全ての電子メールに、送信元のアドレスを付加する手段とを備える電子メールサーバから電子メールを受信する装置であって、受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対しての処理方法を設定する手段を備えることを特徴とする。

【００１１】本発明の第１の側面における方法は、悪戯メールを防止する方法であって、（ａ）受信した電子メールからメールアドレスを抽出するステップと、（ｂ）特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録するステップと、（ｃ）該受信した電子メールのメールアドレスと該ステップ（ｂ）で記憶されたメール

5

アドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するステップとを備えることを特徴とする。

【００１２】本発明の第２の側面における方法は、電子メールを受信する受信手段と、受信した全ての電子メールに、送信元のアドレスを付加する手段とを備える電子メールサーバから電子メールを受信する方法であって、受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対しての処理方法を設定するステップを備えることを特徴とする。

【００１３】本発明によれば、電子メールサーバ側、あるいは、電子メールサーバから電子メールを受信するクライアント側において、簡単な方法で、使い捨てのメールアドレスを作成したり、特定の相手専用のメールアドレスを作成したり、受信者にしか分からない暗号化された情報を含んだメールアドレスを作成することができる。従って、不本意な相手からのメールを簡単に見分けることができ、受け取りたいメールだけを簡単に受け取ることができるようになる。

【００１４】

【発明の実施の形態】図１は、本発明の第１の実施形態を示す図である。同図（ａ）は、サーバの機能構成を示した図である。

【００１５】メール転送サーバ１（以下、サーバ１と記載）は、ある一定のフォーマットに該当するメールアドレスを全て特定の人に送るようにする。例えば、メールアドレスが

ueda@xxxxx.server.com

あるいは、ueda.xxxxx@server.com

のようなフォーマットのメールについて、該メールアドレス内の任意の「xxxxx」に該当するメールに対して登録されたメールアドレスへの転送、もしくは該メールに対して登録された特定のメールボックスへの配送を行う。

【００１６】「xxxxx」の部分に任意の長さの文字を許すようにすれば理論的に無限のメールアドレスが可能であり、十分に長い固定長の文字列を許すようにしても非常に多数のメールアドレスから一つのメールボックスへの配送ができる。

【００１７】このことにより、ユーザは自分が受け取ると決めた「xxxxx」を含まないメールアドレスに対するメールを拒否／消去することが簡単にできるようになる。通常の使用では、メールのユーザは自分にメールを出す可能性がある人に対してそれぞれ異なったメールアドレスを通知し、該通知した全てのメールアドレス以外のメールアドレスに届いたメールは捨てるか無視すればよい。

【００１８】このようにすれば、もしもあるメールアドレスがＳＰＡＭの対象になっていると分かった場合、それまで使っていたメールアドレスを単に使わなくするだけで良く、そのメールアドレスで送ってくるはずだった人がＳＰＡＭを出したか、ＳＰＡＭを出す人にメールアドレスを漏らしたことが分かる。

6

【００１９】また、ホームページ上でニュースを掲載する場合などで、責任の所在を明確にするために自分のアドレスを公開しなくてはならない場合には、一通毎に異なったメールアドレスを用い、かつ、返事の中に特定のキーワードを書いてもらったメールについてのみ返事を受け付けるようにすれば、そのようにして知ったメールアドレスを集めてもＳＰＡＭを送ることはできなくなる。

【００２０】ユーザは、あらかじめサーバ１に対して受信するメールのアドレスの登録をし、該受信メールの送信先として、自分宛のメールアドレスを取得してあるものとする。このメールアドレスを仮に「name@server」とする。

【００２１】サーバ１は、無限個のメールアドレスを用意するために以下のどちらかを行う。

１）name部分に使わない文字（例えば「.」）を用いて「name.任意の文字列@server」宛のメールを全て「name@server」宛のメールとして扱い、必要に応じて、再配布あるいは、メールボックスに入れる。

【００２２】２）Domain Name Service のＭＸ（Media eXchange）フィールドを用いて「name@任意のドメイン名.server」宛のメールをサーバ１で受け取る旨を、世界中に通知し、その受け取ったメールを全て「name@server」宛のメールとして扱い、必要に応じて、再配布あるいは、メールボックスに入れる。

【００２３】更に、サーバ１は、メール受け付け部３において、送信されてきたメールのアドレスあるいはアドレスパターンの照合を行った後、メールを再配布あるいはメールボックスに入れる際に、前もって与えられたユーザからの指示に従って、メールの破棄、エラーメールを送出することによるメールの拒否、あるいは、ユーザのメールリーダソフトが処理できるような何らかのフィールドの追加などの処理をする。この何らかのフィールドの追加処理では、例えば、米国特許５３７７３５４号のような装置を使って、ユーザが容易に無視したり破棄したり、更には読む際の優先度を低くできるようにする。

【００２４】ユーザは、サーバ１に対して、指示を行う際に以下のような処理を実施する手段のどれか一つ以上あるいは全てを持つ。

・ある特定のメールアドレスと処理方法を指定し、それ以降そのメールアドレスに届いたメールはその方法で処理する。

・ある特定のメールアドレスのパターンとその処理方法を指定し、それ以降そのパターンにマッチするメールア

ドレスに届いたメールはその方法で処理する。
・全てのメールアドレスに対して処理方法を指定し、それ以降の全てのメールはその方法で処理する。
【００２５】このために、サーバ１の内部に、指定されたアドレスとそのアドレスに対応する処理方法とを対にして記憶する処理内容記憶部２を設ける。同図（ｂ）は、処理内容記憶部２に記憶されるテーブルの例である。このテーブル２ａの１行は、アドレス又はアドレスパターンを格納するフィールド、該アドレス又はアドレスパターンに対応する処理方法を格納するフィールド、及び該処理方法に於いて使用される処理方法のパラメータなどを記憶するオプションを記憶するフィールドからなる。サーバ１は、届いたメールのアドレスをテーブル２ａに登録されている指定されたアドレス、アドレスパターンと照合し、テーブル２ａ内にマッチするアドレス、または、アドレスパターンが存在する場合、そのマッチしたアドレスあるいはアドレスパターンに対応する処理を行う。また、全てのメールアドレスに対して処理が指定されている時は、そのユーザへ届いた全てのメールに対して処理を行う。
【００２６】サーバ１はまた、ユーザが処理方法の登録／参照を行うための入出力部４を有しており、ユーザから、入出力部４を介して処理方法のリストの参照要求があった時は、そのユーザ名に対応する全ての処理方法のリスト（アドレスパターン、オプションを含む）をユーザに提示する。また、同じく、入出力部４を介するユーザからの処理方法の登録に際しては、
・古い登録の消去、
・登録内容の変更、
・新規の登録
を行う。
【００２７】アドレスパターンの検索の順序が意味を持つようにすることで、複数のアドレスパターンが一つの宛先に対してマッチする場合に前にあるパターンを優先的に使う事で曖昧性なく処理を実行できるようにすることができる。すなわち、マッチする範囲が狭いように指定できる様にする。これにより、例外的なパターンや、前に、一般的なパターンを後に指定できる様になる。この場合には、サーバ１は、ユーザから入出力部４を介して入力される、登録された処理方法の順位の変更（何番目にそのパターンを調べるか）要求、も受け付けるようにする。
【００２８】あるいは、曖昧な場合には登録を受け付けないようにしたり、あるいは、曖昧な場合にはサーバ１の方で適当にマッチする一つの処理方法を選んで処理するようにしても良い。
【００２９】図２は、上記構成のサーバ１により実行される検索の順序が意味を持つ場合の処理の一例を示す図である。サーバ１が電子メールを受信し、メール受付部３においてアドレス、あるいは、アドレスパターンの照

合を行った結果、その電子メールの信用度が曖昧である場合には、特定の処理を行うようにする。同図（ａ）は、サーバ１のメール受付部３がメール受信時に行う処理を示す図である。
【００３０】処理の方法としては、以下のどれか一つ、あるいは、全てを行う。
・通常通り配送を行う。
・単に配送をしない。
【００３１】配送処理をしないという処理方法に該当するアドレスにメールが届いた場合、この場合、サーバは何もしない。同図（ｂ）は、上記の場合に処理内容記憶部２に記憶されるテーブル２ａの内容の例を示している。
【００３２】この場合、アドレス又はアドレスパターンのフィールドに、特定のアドレスあるいは、アドレスパターンを記憶し、対応する処理方法のフィールドには、「捨てる」という処理内容を記録する。オプションは特になしとしている。サーバ１は、該処理内容がテーブル２ａに登録された電子メールを受信すると、同図（ｂ）のテーブル２ａを参照し、該当する処理方法を読みとって、上記電子メールを「捨てる」処理を行う。実際には、電子メールを配送せず、単に何もしなければ、電子メールがメールボックスから自動的に消えてしまう。
【００３３】図３は、受信した電子メールが所定のアドレスあるいはアドレスパターンに一致した場合にエラーメールを送出して拒絶するときのサーバ１の処理と、その場合に、処理内容記憶部２に記憶されるテーブル２ａの内容を示す図である。
【００３４】同図（ａ）は、サーバ１のメール受け付け部３の処理を示した図である。届いたメールのアドレスあるいはアドレスパターンが、テーブル２ａに登録されている特定のアドレスあるいはアドレスパターンと一致した場合、サーバは通常の宛先不明のアドレスが見つかった場合と同様にエラーメールを作成し、それをメールの送付元に送りつける（エラーメール送出）。
【００３５】エラーメールは、実際に送受信中にエラーが発生したと同じように作成され、ＳＰＡＭと思われるメールを受け取った時に、送信元に対して返送するため、ＳＰＡＭの送信者に、メールを送った相手のアドレスが間違っていたなどと思わせる。
【００３６】同図（ｂ）は、上記エラーメール送出処理を実現するためにサーバ１の処理内容記憶部２に記憶されるテーブル２ａの内容例を示す図である。特定のアドレスあるいはアドレスパターンに対して、処理方法として「エラーメール送出」を登録しておく。この例ではオプションは特に無しとしているが、エラーメッセージに含まれる言葉のオプションを登録しておき、エラーメッセージを生成する際に、これらの言葉のオプションから任意に選択して利用するようにすることも可能である。
【００３７】図４は、サーバ１が通常のようにメールは

配送するが、メッセージ中に指定された目印を加える処理を行う場合のメール受け付け部３の処理、処理方法記憶部２のテーブル２ａの登録内容及び目印の例を示した図である。

【００３８】同図（ａ）は、サーバ１のメール受け付け部３の処理を示す図である。処理方法として「目印の付加」を指定する場合は、どんな目印を付加するかユーザが指定する。指定された目印はサーバ１の処理方法のオプションとして処理内容記憶部２に記憶される。従って、同図（ｂ）に示されるように、処理方法記憶部２に記憶されるテーブル２ａには、特定のアドレスあるいはアドレスパターンに対応して、メールに目印を付加する処理方法を採用することが登録されると共に、オプションのフィールドに目印の付加方法（どのようなメッセージを付加するかに関する情報）が登録される。

【００３９】この処理方法に該当するアドレスのメールが届いた場合、サーバ１は、届いたメールに対して、指定された目印を加えた後、通常のメールと同様の配送を行う。

【００４０】同図（ｃ）は、目印の付け方の一例を示した図である。同図では、メール５のヘッダ部５ａに“X-possibly-spam:true”という目印を付ける例を示している。このようにすることによって、ユーザは、届いたメールがＳＰＡＭであるか否かを判別することができる。また、このメッセージを元に、クライアント側で、当該メールを破棄するようにしても良い。目印の付け方は、従来の項で参照した文献を参照されたい。従って、詳細は省略する。

【００４１】図５は、サーバ１が通常のようにメールは配送するが、届いたメールアドレスをメッセージ中に加える場合の処理手順、テーブル２ａの内容、処理例を示した図である。

【００４２】同図（ａ）は、サーバ１のメール受け付け部３の処理を示す図である。また、同図（ｂ）は、処理内容記憶部２に記憶されるテーブル２ａの内容例を示す図である。

【００４３】同図（ｂ）に示すように、届いたメールのアドレスの処理方法として送付宛先を付加する処理が指定されている場合、サーバ１は、その届いたメールに対して、例えば、ヘッダ部分の決まったフィールドに、
X-Forwarded-From: 届いたアドレス
のような形式でアドレスを追加した後、通常のメールと同様の配送を行う。

【００４４】同図（ｃ）は、メール６のヘッダ部分６ａに上記形式でメールを送信してきた相手のアドレスを書き込んで送付先のクライアントへ該メール６を送信する処理形態を示した模式図である。

【００４５】同図（ａ）に示されるように、サーバ１のメール受け付け部３は、メールを受け取ると、そのメールの送り主のアドレスを同図（ｂ）のテーブル２ａに登録されているアドレスあるいはアドレスパターンと照合し、一致しない場合には、通常のメール処理を行うが、一致した場合には、テーブル２ａの一致した行の処理方法のフィールド及びオプションのフィールドを参照して、処理を決定する。今の場合、処理方法は、「送付宛先を付加」であり、オプションは「なし」なので、メールのヘッダ部などの予め決められた部分に上記したようなメッセージを添付してクライアントに送付する。クライアントは、受信メールのこの予め決められた部分に記載されている送り主の記載を見て、破棄するなり、受信することができる。送り主のアドレスを参照して、そのメールを破棄するかしないかを自動的に判断し、当該処理を実行するプログラムをクライアント側に設けておくことも可能である。

【００４６】同図（ｃ）の例では、メール６のヘッダ部６ａに「X-Forwarded-Form：ueda.xxx.xxx@fuji」が添付されている。添付のための具体的な処理方法は、従来の技術の項で参照した文献を参照されたい。従って、詳細は省略する。

【００４７】図６及び図７は、届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバ１の処理手順と処理方法の記録例を示す図である。

【００４８】この処理方法を指定する場合は、処理方法記憶部２のテーブル２ａに、見分けるべき性質の記述、その性質を持っている場合と持っていない場合の処理方法が登録される。見分けるべき性質と、該性質を持っている場合と持っていない場合の処理方法はオプションとしてテーブル２ａに記憶される。あるいは、サーバ１の振る舞いを一部固定して、上記性質を持っているメールの場合は何もしないで破棄し、持っていないメールの場合は送り主のアドレスを該メールに記載し、処理方法では性質だけを指定させ、具体的な処理は、サーバ１にオプションとして記憶させるようにしても良い。

【００４９】見分けるべき性質は、さまざまなものが考えられるが、メールに関する各種情報のパターンマッチ、例えば、Subject が特定の文字列を含むとか、送出した日付が一定の期間内にあるかどうか、あるいは、本文中に特定の文字列が含まれるかどうかなどが考えられる。

【００５０】この処理方法に該当するアドレス宛のメールが届いた場合、サーバ１のメール受け付け部３は、そのアドレスに対応した見分けるべき性質を取り出し、次にそのメールが特定の性質を満たしているかどうか調べ（ステップＳ１０：図６及び図７）、性質が満たされているか否かを判断する（ステップＳ１１：図６及び図７）。次に、満たしている場合は、そのための処理を（ステップＳ１２、Ｓ１２’）、そうでなければそうでない方の処理を（ステップＳ１３、Ｓ１３’）、処理方法記憶部２のテーブル２ａのオプション・フィールドあ

るいはサーバ１の固定情報記憶域から取り出し、該当する処理を行う。この処理の方法は、前述した処理方法のいずれであっても良いし、サーバ１によっていくらか制限を加えても良い。あるいは、後述するような処理でも良い。

【００５１】図８及び図９は、処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバ１はそれを解釈して実行する場合のサーバ１の処理手順とサーバ１に記憶されるデータを示す図である。

【００５２】図８（ａ）及び図９（ａ）は、サーバ１の処理手順を示す図であり、図８（ｂ）は、暗号解読用の鍵を記憶するテーブル４であり、図８（ｃ）及び図９（ｂ）、（ｃ）は、処理方法記憶部２のテーブル２ａの内容例を示す図である。

【００５３】ユーザはこの処理方法を指定する前に暗号解読の鍵をサーバ１に登録する。鍵はサーバ１の種類に応じて、ユーザ毎に指定するようにしても良いし（図８（ｂ）参照）、アドレスパターン毎に変えるようにしても良い。すなわち、前者ではユーザ毎のオプションとして暗号解読の鍵を保存し（図８（ｂ））、後者では処理方法のオプションとして鍵を保存する（図８（ｃ））。

【００５４】また、ユーザがこの処理方法を指定する場合、暗号化されたコマンド部分を取り出すためのパターンを指定し、それはオプション、アドレスパターンの一部、またはオプションの一部もしくは処理方法の一部としてサーバ１内部のテーブル２ａに保存される（図９（ｂ）、（ｃ））。

【００５５】ユーザはメールアドレスを知らせる際に処理すべきコマンドをサーバ１が解釈できるような文字列で表現し、次にその文字列を暗号化する。そして、該暗号化されたコマンドとこの処理方法を、指定したアドレスパターンに適合するような形式にして、メールアドレスの任意の文字列の部分に加えて、最終的にメールアドレスを作成し、このメールアドレスをサーバ１に知らせる。

【００５６】サーバ１のメール受け取り部３は、この処理方法に該当するアドレスにメールが届いた場合（ステップＳ１５で、照合した結果、一致を見た場合）、まず、内部に保存された暗号化されたコマンド部分を取り出すためのパターンを取り出し、それに従って、上記アドレスから暗号化されたコマンド部分を取り出す（ステップＳ１６）。そして、そのコマンド部分を入出力部４内に予め保存されている当該鍵を用いて解読し（ステップＳ１７）、次に解読された文字列（コマンド）を解釈して処理を行う（ステップＳ１８）。処理は上述されたどの方法をとっても良いし、サーバによっていくらかの制限を加えても良い。また、サーバによっては適当なプログラミング言語（例えば、Perl）の処理系と連係することでより高度の処理を行っても良い。

【００５７】また、図５のサーバ１は、常に全てのメールアドレスに対してメールを配送し、予め、テーブル２ａに登録されている該当アドレスのメールについては、届いたメールアドレスをメッセージ中に加えるという操作をするが、サーバ１にこのような機能を持たせつつ、入出力部４からの指示を一切受け付けないようにすることもできる。このようにすると、メールアドレスによって処理方法を変える必要がないので、サーバ１の方でユーザの指定方法を受け付ける構成要素とアドレスあるいはアドレスパターン毎に行う複雑な処理が不要となり、サーバ１の負荷を大幅に減らすことができる。

【００５８】なお、理論的に無限通りのアドレスを一つのアドレスに対応させ、メールを届けることは既知の技術であるが、届いたアドレスをメール内に付加することで、悪戯メールに対処できるようにすることが本願の新しい技術である。

【００５９】前述の説明では、サーバ１に処理をさせていたが、サーバ１を使ったのと同じ効果を得るのに、負荷の重いサーバでなくクライアント側で処理を行うような構成にすることも可能である。また、あらかじめ暗号鍵を公共の通信路を通して送るのは危険であるが、クライアントに暗号鍵など上記暗号化の処理に必要な情報を全て置くことでこの危険をなくすことができる。

【００６０】図１０は、クライアントに悪戯メール防止装置を設ける場合のサーバの処理を説明する図である。この場合、サーバ１０は、メールを受信すると、メールの送り相手のアドレスをメール内の、例えば、ヘッダ部に記録した後、通常のメール処理を行う。通常のメール処理とは、受信メールのクライアントへの配信などである。

【００６１】クライアントで処理をする場合は、サーバで行う「通常のメールと同様の配送を行う」処理を、クライアント側で「通常のメールと同様に表示する」処理に置き換えて実行するようにする。

【００６２】図１１は、クライアント側で悪戯メールの処理を実行する場合のクライアントの構成を示す図である。まず、クライアント２０は、メールを取り込むと、そのアドレスを見て、処理方法記憶部２２内のテーブル２２ａに記憶されているアドレスあるいはアドレスパターンと一致するか否かを判断する。一致しない場合には、メール表示／作成装置２１において、メールの表示を行う。また、照合の結果、一致した場合には、処理方法記憶部２２に記憶されているテーブル２２ａの処理方法、オプションの各フィールドを参照して、前述したサーバ１と同様な処理を行う。メールを作成する場合には、ユーザがメール表示／作成装置２１を使用して作成する。このとき、処理方法記憶部２２内のテーブル２２ａを参照して、テーブル２２ａに登録された相手にメールを送信する場合には、暗号化したパターンを含んでいるアドレスを送信相手に教えるための処理を行う。

【００６３】更に、クライアント２０の付加機能とし

て、相手が自分にメールを送信するときに発行した自分のアドレスを付加的な情報（発行日時、発行した相手、その他）と関連づけて記録しておくことで、届いたメールのアドレスに対応したそれらの情報を表示するようにすることもできる。このために、付加的情報の表示装置２３が設けられると共に、処理方法記憶部２２内のテーブル２２ａには、各アドレスあるいは各アドレスパターンに対応して、日時や相手の名前などを記録できるようにしておく。これにより、どのような相手からメールアドレスが漏れたのか、事後に調査することが容易に行える。

【００６４】更に、クライアントの付加機能として、発行したアドレスに対して受け取れる相手を関連づけて記録しておくことで、その後そのような相手にメールを出す際には記録されている発行したアドレスを差出人として自動的に用いるようなクライアントを実現することができる。

【００６５】このために、処理方法記憶部２２内のテーブル２２ａのアドレス部（アドレスのフィールド）にパターンでなく特定のアドレスを登録できるようにし、テーブル２２ａ内にオプションとして、受け取りたい相手のメールアドレス（の列）を保存するようにする。

【００６６】メールを作成する際には、送る相手のアドレスと一致するアドレスを受け取りたい相手として持つようなアドレスパターンをテーブル２２ａから検索し、見つかればそれを差出人として使う。複数の相手に同時にメールを送る場合には、それらの送り先全てを受け取りたい相手として持つようなアドレスパターンをテーブル２２ａから検索する。

【００６７】もしも見つからなければ、新しい相手先（あるいはその組み合わせ）なので、以下の１）～３）どれかをユーザに選ばせるか、あるいはシステムが１）～３）の中のいずれかを固定的に選んで動作する。

１）デフォルトのアドレスを使う、

２）既存のアドレスパターンのどれか一つを用いる、

３）新しいアドレスを作り、それと新しい相手先を関連づける。

【００６８】２）の動作をする場合には、相手先（の全て）をそのアドレスパターンの受け取りたい相手としてテーブル２２ａに登録することができる。また、受け取りたい相手以外からのメールを別処理するように構成しても良い。この場合、該別処理としては、処理方法記憶部２２内のテーブル２２ａのオプション部（オプション・フィールド）に指定された動作、あるいは、クライアント２０で固定された動作（例えば、そのメールを捨てる）等が考えられる。

【００６９】あるいは、図１２に示されるように、クライアント２０がエラーメールと同等の内容のメールを作成し（ステップＳ３１）、これを送り主に送り返すようにする（ステップＳ３２）ことも可能である。

【００７０】以下に、サーバ１側で悪戯メールを処理する場合のサーバ１の機能の具体例を説明する。サーバ１は内部に登録された処理方法のリストを持っている（図１（ａ）の処理内容記憶部２及び図１（ｂ）のテーブル２ａ参照）。処理方法のリストはアドレス部（アドレス又はアドレスパターン）、処理方法、オプション部の３つが一組となった情報のリストである。アドレス部は正規表現を用いたパターンで表されるものとし、特定アドレスへのマッチを希望する時には、ワイルドカード文字を使わず、また、全てのアドレスにマッチを希望する時には「ユーザ名．＊」のパターンを保持する。

【００７１】ただし、以下のような制限が課せられてあるものとする。図４の場合は目印はメールのヘッダ部にのみ付加できるものとし、該目印として付加すべきヘッダの文字列を登録する。

【００７２】図６あるいは、図７の場合においては、区別する性質は、メールのヘッダ部の正規表現を用いたパターンマッチとし、見るべきヘッダフィールド名、マッチするパターン（正規表現）、そして、マッチした場合とそうでない場合の処理の内容が再帰的に指定できるものとする。この場合、再帰的な処理内容のオプション部も同時に指定できるものとする。

【００７３】図８及び図９の場合の暗号鍵は処理方法毎に異なっていて良いものとし、これを処理内容記憶部２のテーブル２ａのオプション部に記憶する。また、テーブル２ａのアドレス部に一組の括弧をいれることで、それらで括られた部分を暗号化されたコマンドとして扱うことを示すものとする。サーバ１は復号化されたコマンドの解釈・実行により「メールを処理する」サブプログラム（メール処理サブプログラム）を呼び出すようにする。

【００７４】サーバ１は、メールを受け取った場合、「user．任意の文字列@server.domain」というメールアドレスを全て「user@server.domain」というメールアドレスに届いたものとして扱うものとする。

【００７５】サーバ１はメールを受け取ると、宛先アドレスを「宛先」として記憶し、また「@」より左側の文字列を「拡張ユーザ名」として記憶する。また、拡張ユーザ名の最も左にある「．」よりも左側の文字列を取り出し、この文字列を「ユーザ名」として記憶する。もしも、メールアドレスに「．」が含まれていなければ拡張ユーザ名と同じ文字列を「ユーザ名」として記憶する。

【００７６】次に、拡張ユーザ名と、処理方法のリストの各アドレス部とを順に照合し、マッチするかどうか調べる。もしもどれともマッチしなければ、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。

【００７７】もしもどれかとマッチした場合、そこに記述された処理方法とオプションに従って、メールを処理する。

15

＜メール処理サブプログラムのアルゴリズム＞メール処理サブプログラムの呼び出し形式は、次の通りである。括弧内は引数。

【００７８】サブプログラム：メールを処理する（処理方法、オプション、メール、拡張ユーザ名、ユーザ名、宛先）

メール処理サブプログラムの機能は、次の通りである。

・処理方法が、「mail」の場合、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。

・処理方法が、「dispose 」の場合、単にそのメールを捨てて処理を終了する。

・処理方法が、「error 」の場合、通常処理の中の宛先不明の場合のエラーメール送出のルーチンに行き、該ルーチンの実行によりエラーメールを送出する。

・処理方法が、「header」の場合、オプション部に記憶されている、目印の文字列をメールのヘッダ部に付け加え、「ユーザ名@server.com 」宛のメールとして、通常の配送処理を行う。

・処理方法が、「mark」の場合、メールのヘッダ部分にX-forwarded-from：宛先

という文字列をつけ加え、「ユーザ名@server.com 」宛のメールとして、通常の配送処理を行う。

・処理方法が、「if」の場合、オプション部は以下の項目がつながった文字列であるとする。

・ () で括られた調べるべき性質

・ {} で括られている、上の性質を満たしたときの処理方法とオプション

・ {} で括られている、上の性質を満たさないときの処理方法とオプション

調べるべき性質には、以下のいずれかあるいは、それらを＆＆、｜｜、またはつりあった () で括って任意個連結したものとする。

・フィールド名：受理パターン

・フィールド名！非受理パターン

・date　before　日付

・date　after 日付

ただしパターンは正規表現とする。

【００７９】フィールド名はメールのヘッダ部にあるフィールド名で例えばFromあるいは、Subject のようなものである。処理方法とオプションは、メール処理サブプログラムで処理できる処理方法とそのオプションが空白で区切られて並んでいるものとする。ただしオプションがない場合には空白がない場合を許可する。

【００８０】まず、オプション部から以上のフォーマットされた文字列から調べるべき性質を取り出し、それに従って届いたメールのヘッダを調べる。調べるべき性質が「フィールド名：受理パターン」の場合は、メールからそのフィールド名の内容をメールから取り出しそれが受理パターンとマッチする場合のみ真となりそれ以外は偽となる。

16

【００８１】調べる性質が「フィールド名！非受理パターン」の場合は、メールからそのフィールド名の内容をメールから取り出しそれが受理パターンとマッチしない場合のみ真となりそれ以外は偽となる。

【００８２】調べるべき性質が「date　after 日付」の場合は、メールのDateフィールドを解釈し、また「日付」部分の日付を解釈しDateフィールドの日付が指定の日付より後の場合のみ真となりそれ以外は偽となる。

【００８３】調べるべき性質が「date　after 日付」の場合は、メールのDateフィールドを解釈し、また「日付」部分の日付を解釈しDateフィールドの日付が指定の日付より後の場合のみ真となりそれ以外は偽となる。

【００８４】調べるべき性質が「date　before　日付」の場合は、メールのDateフィールドを解釈し、また「日付」部分の日付を解釈しDateフィールドの日付が指定の日付より前の場合のみ真となりそれ以下は偽となる。

【００８５】調べるべき性質が＆＆、｜｜、 () で結合されている際には、＆＆は論理積、｜｜は論理和で論理積の結合力が強いものとして扱い、 () は通常と同じように優先的に結合して計算するようにして調べる。

【００８６】次に、調べた結果の真偽によって、二つの処理方法を選ぶ。処理方法から最初の空白まで（あるいは空白が無ければその全て）を処理方法とし、残りをオプションとして、再帰的にメール処理サブプログラムを呼び出す。

【００８７】例えば、オプション部には以下のような記述が可能である。

(Subject:.Hello.* &&From!friendname@some.domain)[if(From: spammer)[error][header greeting:true]][mail]

この場合、メールのSubject がHello を含みFromがfriend__name@some.domainを含まない場合は、ifで始まる部分が処理方法となり、再帰的にifの処理が行われる。それ以外の場合は通常のメール配送処理が行われる。

・処理方法が、「decrypt 」の場合、まず、アドレスパターンの括弧で括られた部分とマッチする文字列を取り出し、この文字列を「暗号化されたコマンド」とする。次にオプション部から暗号の鍵を取り出し、この鍵を用いて暗号化されたコマンドを復号化する。そして、得られた文字列のうち、最初の空白までを処理方法、残りをオプションとしてメール処理サブプログラムを再帰的に呼ぶとする。

＜処理方法のリストの登録／参照＞サーバ１はまた、処理方法のリストの登録／参照手段（図１（ａ）の入出力部４）を持っており、ユーザから、処理方法のリストの参照要求があった時は、そのユーザ名に対応する処理方法、すなわち「ユーザ名」というアドレス、あるいは「ユーザ名．」で始まるパターンを持った全ての処理方法のリスト（アドレスパターン、オプションを含む）をユーザに提示する。

【００８８】処理方法の登録に際しては、
・古い登録の消去
・登録された処理方法の順位の変更（何番目にそのパターンを調べるか）
・登録内容の変更
・新規の登録
が行えるようになっている。
＜処理方法の登録＞サーバ１は、アドレス名、（サーバ１が解釈できる）コマンド、コマンドのオプションを受け取って、これらをユーザの登録された処理方法のリスト（図１（ａ）の処理内容記憶部２のテーブル２ａ）に加える。
【００８９】具体例
・add アドレス　コマンド名　［オプション］
コマンド名は“dispose ”、“error ”、“mark”、“header”、“if”、“decrypt ”、“mail”のどれかを使用する。
【００９０】アドレス、コマンド名、オプションは空白で区切られ、それらをサーバ１は分離して、文字列としてユーザにより登録された処理方法のリストとしてテーブル２ａに記憶する。
【００９１】ユーザ指定の処理方法がすでにあるときは、新たに追加されたものはリストの最後に置く。“dispose ”、“error ”、“header”はオプションを持たない。
【００９２】“mark”コマンドは付加ヘッダ名をオプションとして持つので、サーバ１は以下のようなコマンドを受け付ける。
add アドレス　mark　ヘッダ名　ヘッダ内容
（例えば、add　ueda.broadcast　mark　X-Possibly-Spam：　true）
を受け付け、ヘッダ名（X-Posibly:）とヘッダ内容（true）を文字列としてつなげて、これをオプション部として扱う。
【００９３】“if”コマンドはチェック内容とその後の動作をオプションとして与える。オプション文字列は、メール処理サブプログラムのオプション部で受け付けられる構文とする。
【００９４】非合致時の動作内容は省略でき、その場合、デフォルトとしてerror コマンドが指定されたものとして、オプション文字列に加えてテーブル２ａに記憶する。合致時の動作内容も省略でき、その場合デフォルトとしてmailコマンドが指定されたものとしてテーブル２ａに記憶する。ただし非合致時の動作を指定するときは合致時の動作内容は省略できない。
【００９５】登録時の構文は、add のコマンドとオプションを合わせたものである。サーバ１が受け取るコマンドは、例えば、以下のようになる。
add　ueda.from.friends　if　（From：friend１@his.domain　|From：friend２@her.domain）

add　ueda.１month.from.990401　if　（date　before　1999/5/1）｛mail｝｛error｝
add　ueda.report　if　（Subject　：.*bug.*report*）｛if（From：customer1　|From：customer2｝｛mark　X-customer-report　：yes｝｛mark　X-bug-report：yes｝｝｛mail｝
サーバ１はこれらのコマンドを受け取り、オプション部分の全ての文字列をユーザの指定として加える。
【００９６】“decrypt ”コマンドはアドレスパターン中に＼（＼）で括られた複合可能部分を含むパターンを指定し、その他にオプションとして復号鍵を受け取る。パターンの正規表現は通常と異なり、“.”、“＊”は＼でエスケープされている場合、初めてワイルドカード文字として扱われる。
【００９７】サーバ１が受け取るコマンドは例えば下記のようになる。
add　ueda.commandkey1.＼（＼.＼＊＼）decrypt　NsaOghzaldvaJAgalAsfD034J
復号化された文字列はadd のコマンドとオプションを合わせた文字列である。
＜処理内容の参照＞ユーザ名を与えてその登録された処理方法のリストを返す。
【００９８】具体例
show　ユーザ名
をサーバ１に送ると、ユーザ名. で始まる登録された処理方法のリストの内容を全てテキストで送り返す。
【００９９】送り返される内容は、登録時の構文の内、add を除いたアドレスパターン以降のフォーマットとする。
＜処理内容の消去＞アドレスパターンを与えて、それと全く同じ内容のパターンを検索し、相当する項目をリストから消去する。もしも見つからなければエラーを返す。
【０１００】具体例
delete　パターン
パターンと完全に一致する項目がテーブル２ａ内にあれば、その項をテーブル２ａから消去し、消去する前の内容をshowと同様にテキストで送り返す。もしも見つからなければ、その旨のエラーメッセージをテキストで送り返す。
＜処理内容の変更＞アドレスパターンとそこでの変更内容であるコマンド（とそのオプション）を与えて、現在登録されている処理方法と入れ替える。
【０１０１】具体例
replace パターン　コマンド名［ オプション］
構文はadd コマンドと全く同じである。パターンと完全に一致する項目があれば、その項のコマンドとオプションを変更処理で指定されたコマンド名とオプションで入れ替える。そして、入れ替える前の情報をdeleteと同様にテキストで送り返す。もし、パターンが見つからなけ

れば、add と全く同じに動作し、元のパターンが見つからなかった旨の警告をテキストで送り返す。

＜変更処理の内、順序入れ替えに関するもの＞アドレスパターンとそのパターンを検査する順序を指定し、その指定された順序に指示パターンを移動させる。

【０１０２】具体例

order パターン　順番

パターンと完全に一致する項目があれば、その項を前から数えて指定された順番で検査されるように、指定のリストの順序を変更する。この変更によって、それ以降の検査は一つずつ検査の順序が後ろにずれるようにする。もしも一致する項目がなければ、パターンが見つからなかった旨のエラーをテキストで送り返す。

＜メールアドレス作成部（クライアント２０にある独立したプログラム）＞メールの作成で暗号化する場合、クライアント２０のプログラムは、ユーザに対して、チェックするフィールド名又は日付を問い合わせる。図１３は、クライアント２０のプログラムが、ユーザにフィールド名や日付を問い合わせるユーザ・インタフェース画面３０のフォーマットの一例を示している。

【０１０３】これに従い、非受理のボタン３１がチェックされていたら、

フィールド名！パターン＆＆

受理のボタン３２がチェックされていたら、

フィールド名：パターン＆＆

日付のfromフィールド３５に入力があれば、

Date　from　日付

日付のtoフィールド３６に入力があれば、

Date　after 日付

を文字列にしてつなげコマンドとする。

【０１０４】Subject, to, From に対応して、パターン３７～３９を使用する。

＜サーバとクライアントの組み合わせ＞上記説明では、サーバ１が悪戯メールの処理を行う主旨で説明したが、前述したように、クライアント２０側で悪戯メールの処理を行うことも可能である。この場合、図１０のサーバ１０と、例えば図１１のような、図２～図９のサーバ１の機能を有したクライアント２０とを組み合わせることができる。

【０１０５】サーバ１０はメールを受け取ると、メールアドレスの「@」より左側の文字列を調べ、メールアドレス内に「．」が含まれていなければ通常の配送処理（ユーザ名不明の場合のエラーメール送出を含む）を行う。一方、「．」が含まれていなければ、宛先のアドレスを「宛先」として記憶し、また、最も左にある「．」よりも左側の文字列を取り出し、それを「ユーザ名」として記憶する。

【０１０６】そして、受信メールのヘッダ部分に、例えば、

X-Forwarded-From：宛先

という文字列を付け加え、「ユーザ名@server.com 」宛のメールとして、通常の配送処理を行う。X-Forwarded-Fromという部分は、クライアントが処理できさえすれば、どの様な文字列に変更しても良い。

【０１０７】クライアント２０（図１１参照）に存在するメール表示／作成装置２１は、前述の例と同様に処理方法のリストを持っているものとする。ただし、クライアント２０の場合では更に、各々の登録されたアドレスに関する補助的な情報（例えば、最初に登録した日時、相手の氏名その他覚書）や相手として用いるアドレスを蓄えることができるものとする。また、通常の処理として、メールの表示あるいはフォルダへの保存、破棄、作成（発送）を行えるものとする。

【０１０８】クライアント２０はサーバ１０からメールを受信すると、その中の

X-Forwarded-From：宛先

というヘッダに注目し、その宛先を用いて、上記の例と同様の処理をする。ただし、上述したサーバにおける「通常の配送を行う」処理に関しては、クライアント２０では、通常の処理の一部として、メールの表示あるいはフォルダへの保存を行うものとする。

【０１０９】エラーメールの配送に関しては、クライアントは通常そのような機能を有する手段を持たないので、標準的なエラーメールのフォーマットを内部的に保持しておき、それを用いて、エラーメールの送出を行うものとする。

【０１１０】クライアント２０はまた、処理方法のリストの登録／参照手段（不図示、図１の入出力部４に対応する手段）を持っており、ユーザから、処理方法のリスト（処理方法記憶部２２に記憶されているテーブル２２ａの登録内容）の参照要求があった時は、全ての処理方法のリスト（アドレスパターン、オプション、補助情報を含む）をユーザに提示する。

【０１１１】処理方法の登録に際しては、

・古い登録の消去

・登録された処理方法の順位の変更（何番目にそのパターンを調べるか）

・登録内容の変更

・新規の登録

が行えるようになっている。

【０１１２】クライアント２０はまた、通常のメールの作成にあたり、処理方法の中にワイルドカード文字を使っていないアドレスパターンに対応した相手のアドレスが登録されている時には、そのアドレスパターンを差出人のアドレスとして使うようにすることができる。

【０１１３】このために、送る相手のアドレスと一致するアドレスを処理方法の受け取りたい相手として持つようなアドレスパターンを検索し、見つかればそれを差出人として使う。複数の相手に同時にメールを送る場合には、送り先全てを受け取りたい相手として持つようなア

ドレスパターンを検索する。

【０１１４】もしも見つからなければ、新しい相手先（あるいはその組み合わせ）なので、以下のどれかをユーザに選ばせる。

１）デフォルトのアドレスを使う、

２）既存のアドレスパターンのどれか一つを用いる、

３）新しいアドレスを作り、それと新しい相手先を関連づける。

【０１１５】２）の動作をする場合には、相手先（の全て）をそのアドレスパターンの受け取りたい相手として登録するかどうか、更にユーザに問い合わせをすることで、次回からメールを送る際に同じ作業をしないようにできる。

【０１１６】

【発明の効果】以上、説明したように、本発明によればサーバ側が簡単な方法で無限ないし大量のメールアドレスを有するメールを一つのメールボックスへ配送するようにしたので、使い捨てのメールアドレスを作成したり、特定の相手専用のメールアドレスを作成したり、受信者にしか分からない暗号化された情報を含んだメールアドレスを作成することにより、不本意な相手からのメールを簡単に見分けることが可能となる。

【０１１７】この結果、ＳＰＡＭと呼ばれる悪戯や宣伝のためのメールを簡単に除外して受け取りたいメールだけを簡単に受け取ることができるようになる。また、このような機能をサーバとクライアントの組み合わせで行う様にすることにより、サーバの改造をほとんど必要とせずに、現在流通している枠組みのサーバにおいても簡単に実現することが可能である。

【０１１８】また、ＳＰＡＭメールを除外するのはサーバでもクライアントのソフトでも容易に行うことができ、かつ必要なメールは決して削除されない。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示す図である。

【図２】受信したメールの信用度が曖昧である場合の処理のサーバにおける処理の一例を示す図である。

【図３】受信した電子メールが所定のアドレスあるいはアドレスパターンに一致した場合にエラーメールを送出して拒絶するときのサーバの処理と処理内容記憶部に記憶されるテーブルを示す図である。

【図４】サーバが通常のようにメールは配送するが、メッセージ中に指定された目印を加える処理を行う場合のメール受け付け部の処理、処理方法記憶部のテーブル及び目印の例を示した図である。

【図５】サーバが通常のようにメールは配送するが、届いたメールアドレスをメッセージ中に加える場合の処理内容、テーブル、処理例を示した図である。

【図６】届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理と処理方法の記録例を示す図（その１）である。

【図７】届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理と処理方法の記録例を示す図（その２）である。

【図８】処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図（その１）である。

【図９】処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図（その２）である。

【図１０】クライアントに悪戯メール防止装置を設ける場合のサーバの処理を説明する図である。

【図１１】クライアントで悪戯メールの処理をする場合のクライアントの構成を示す図である。

【図１２】エラーメールと同等の内容のメールを作成し、これを送り主に送り返す場合の処理を示す図である。

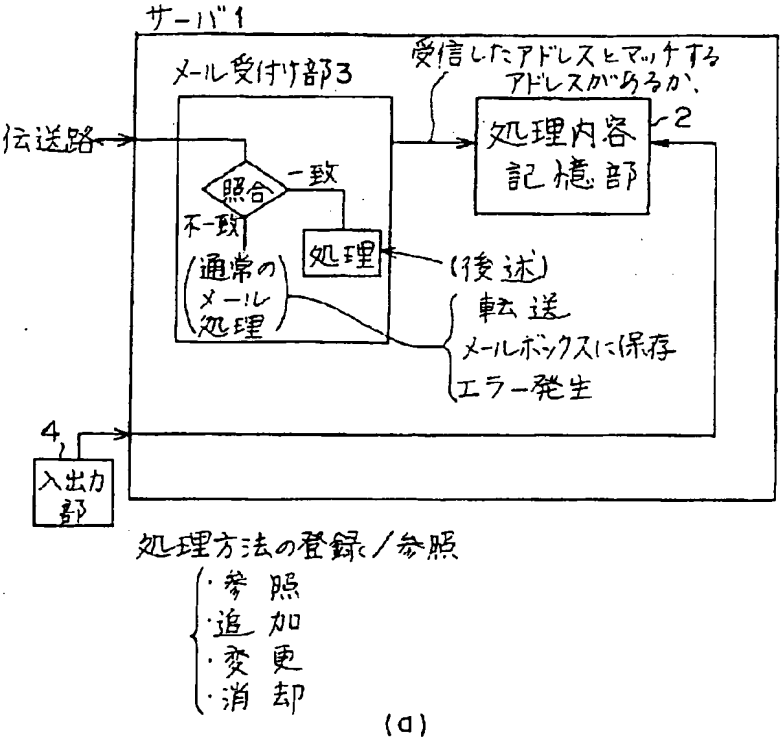
【図１３】クライアントのプログラムが、ユーザにフィールド名や日付を問い合わせるフォーマットの一例を示す図である。

【符号の説明】

１、１０　サーバ
２ａ、４、２２ａ　テーブル
２　処理内容記憶部
３　メール受け付け部
４　入出力部
６　メール
６ａ　ヘッダ部
２０　クライアント
２１　メール表示／作成装置
２２　処理方法記憶部
２３　付加的情報の表示装置
３０　ユーザ・インタフェース画面
３１　非受理ボタン
３２　受理ボタン
３５　from入力フィールド

【図１】

本発明の第1の実施形態を示す図



処理方法の登録／参照
- 参照
- 追加
- 変更
- 消却

(a)

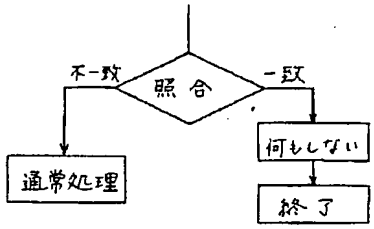
2a

アドレス又はパターン	処理方法	オプション

(b)

【図２】

受信したメールの信用度が曖昧である場合の処理のサーバにおける処理の一例を示す図



(a)

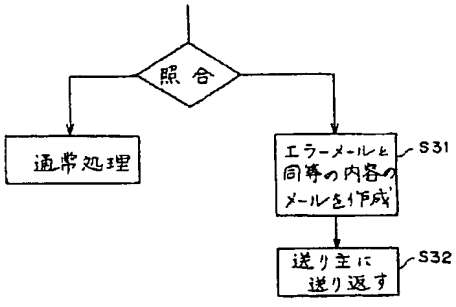
2a

アドレス又はパターン	処理方法	オプション
	捨てる	なし

(b)

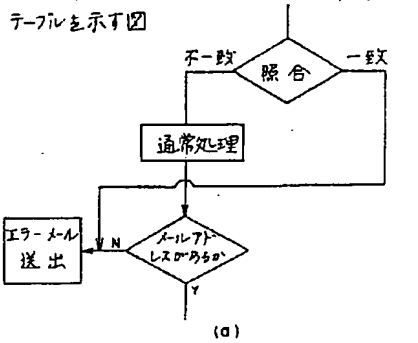
【図１２】

エラーメールと同等の内容のメールを作成し、これを送り主に送り返す場合の処理を示す図



【図３】

受信した電子メールが所定のアドレスあるいはアドレスパターンに一致した場合にエラーメールを送出して拒絶するときのサーバの処理と処理内容記憶部に記憶されるテーブルを示す図



(a)

2a

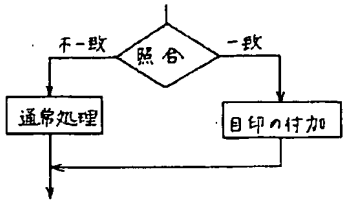
アドレス xはパターン	処理方法	オプション
	エラーメール送出	なし

(b)

【図４】

サーバが通常のようにメールは配送するが、メッセージ中に指定された目印を加える処理を行う場合のメール受け付け部の処理、処理方法記憶部のテーブル及び目印の例を示した図

(a)



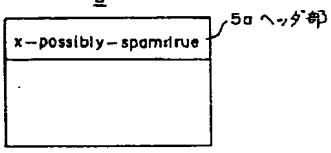
(b)

2a

アドレス xはパターン	処理方法	オプション
	目印の付加	目印の付加方法

(c)

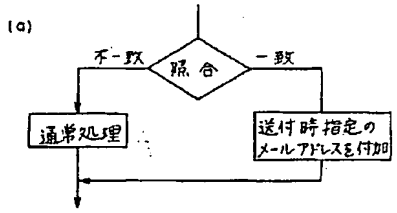
5



【図５】

サーバが通常のようにメールは配送するが、届いたメールアドレスをメッセージ中に加える場合の処理内容、テーブル、処理例を示した図

(a)



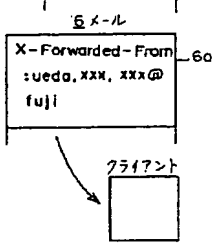
(b)

2a

アドレス xはパターン	処理方法	オプション
	送付先を付加	なし

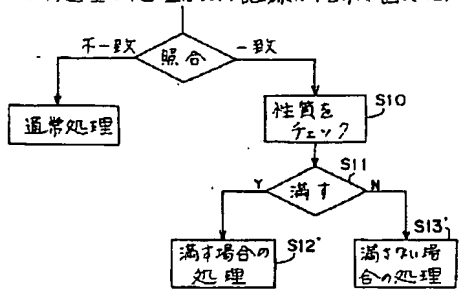
(c)

6 メール



【図７】

届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理と処理方法の記録例を示す図(その2)



(a)

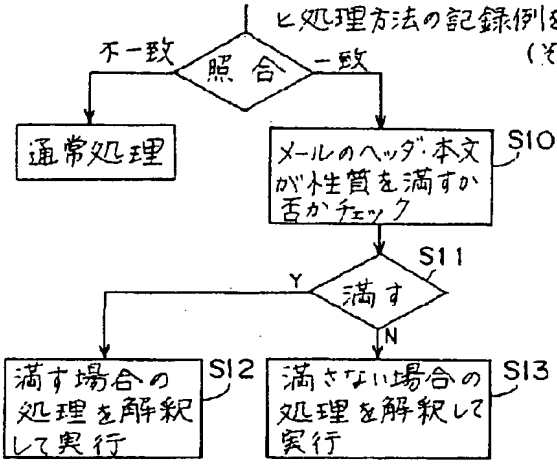
2a

アドレス xはパターン	処理方法	オプション
	性質により処理を変える	性質の記述

(b)

【図６】

届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理方法の記録例を示す図（その１）



(a)

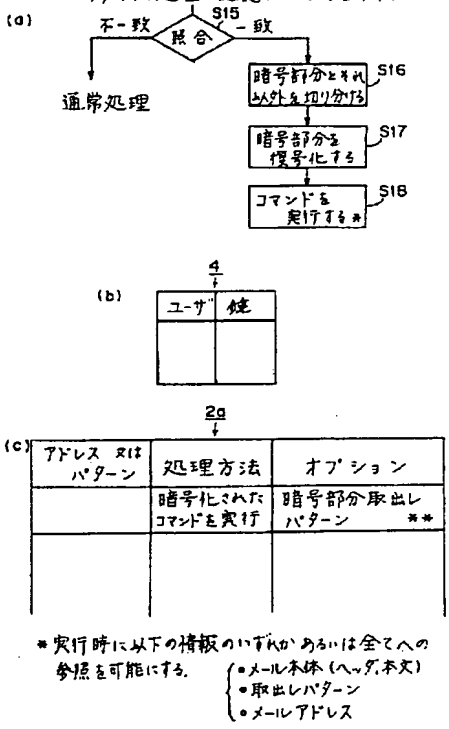
2a

アドレス又はパターン	処理方法	オプション		
	性質により処理を変える	性質の記述	満す場合の処理とそのためのオプション	満さない場合の処理とそのためのオプション

(b)

【図８】

処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図（その1）

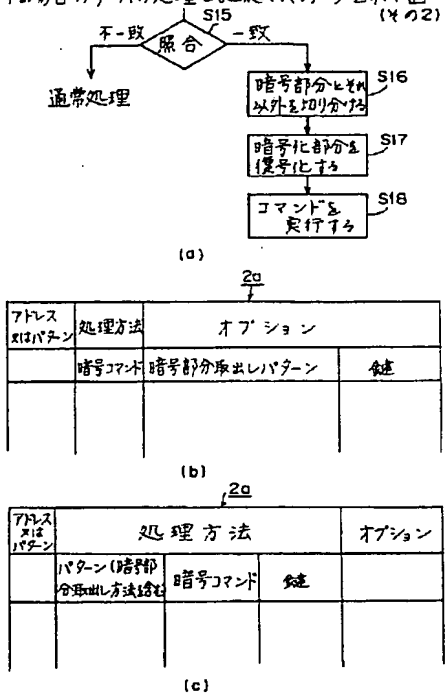


*実行時に以下の情報のいずれかあるいは全てへの参照を可能にする。
- メール本体（ヘッダ本文）
- 取出しパターン
- メールアドレス

**暗号切出しパターンはオプションでなくアドレスパターンの一部として指定保存しても良い。

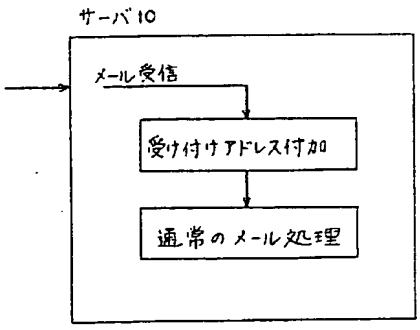
【図９】

処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図（その2）



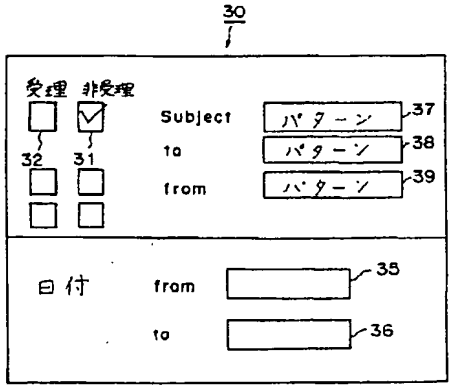
【図１０】

クライアントに悪戯メール防止装置を設ける場合のサーバの処理を説明する図



【図１３】

クライアントのプログラムが、ユーザにフィールド名や日付を問い合わせるフォーマットの一例を示す図



【図１１】

クライアントで悪戯メールの処理をする場合の
クライアントの構成を示す図